UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/534,857	05/13/2005	Sebastien Canard	33901-175PUS	7415

27799 7590 02/27/2009

COHEN, PONTANI, LIEBERMAN & PAVANE LLP
551 FIFTH AVENUE
SUITE 1210
NEW YORK, NY 10176

EXAMINER	
VAUGHAN, MICHAEL R	
ART UNIT	PAPER NUMBER
2431	
MAIL DATE	DELIVERY MODE
02/27/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/534,857	CANARD ET AL.	
	Examiner	Art Unit	
	MICHAEL R. VAUGHAN	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 January 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *13 May 2005* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

The instant application having Application No. 10/534,857 is presented for examination by the examiner. Claims 20 and 21 have been added. Claims 1-21 are pending.

Response to Amendment

Drawings

The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: the steps mentioned on pages 10-11 aren't specified by step numbers in the drawings. Also, the drawings are void of any references which would correlate between the drawings and the written description easier. Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Information Disclosure Statement

The IDS submitted on 1/15/09 has been considered and a copy is attached with this Office Action.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-21are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

As per claim 1, the scope of the phrases "means configured to" is unclear. This does not invoke means plus function under 112, 6th paragraph so it is very much open to interpretation what the means here is. Also, the word fast in the preamble is subjective and relative. Dependent claims are likewise rejected. Appropriate correction is required.

As per claim 3, the newly amended is difficult to ascertain its scope. A series of tokens is defined. Then this series of tokens is references by "one of" and "the others". This indefinite referencing causes a problem when defining the scope of the claim. If

there is but one series of tokens, then there should be no "others". If the intent of the amendment is to address the tokens, then the series need not be recited after the series of tokens is defined. Dependent claims are likewise rejected.

As per claims 9 and 10, it is unclear from the disassociated of the series of tokens how the phrase "lower rank" is attributed a token. No real meaning is given with respect to ranking tokens in claim 3. Examiner cannot ascertain from the claim language any relationship between tokens of than belong to a series. If order or value is intended, that fact needs to be explicitly defined in the claim.

As per claim 15, the same problem exists as mentioned in the rejection of claims 1 and 3. Dependent claims are likewise rejected.

As per claim 16, it is unclear how a "stage" can calculate the series of tokens. As the claim relates to a system, the part of the system which can calculate needs to be defined and attributed this function.

Response to Arguments

Applicant's arguments filed 1/15/09 have been fully considered but they are not persuasive. First with respect to the amendment of a unique anonymous signature which is used for each session; Examiner respectfully disagrees with the allegation that Teper does not teach this limitation. Teper teaches the use of anonymous authentication and signatures during sessions. The term session is generally used to groups a series of transmissions which achieve a specific goal. Sessions timeout for

security reasons and must be renegotiated. It is quite evident when Teper says in column 12, lines 14-16, that the authentication processed is repeated that this explicitly suggests that unique signatures are generated for each session. They are all unique at least being seeded with pseudo-random challenges to begin the process (col. 9, lines 57-59). Then once the anonymous session ID is created (column 11, lines 27-28), Teper explicitly calls it unique. Unique carries a specific meaning in the field of cryptography. Uniqueness means having a very low probability of being repeated or the same. Teper's invention is grounded in security and anonymity. This unique is the basis of the security in conjunction with anonymity between the client and service provider. Examiner finds sufficient support in Teper to suggest this new limitation.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-5, 7-10, and 20 are rejected under 35 U.S.C. 103 as being unpatentable over Teper et al. (US 5,815,665) hereinafter Teper, in view of Camnisch et al. (US 2002/0103999 A1), hereinafter Camnisch.

As per claim 1, Teper teaches the limitation of "identifying and registering a client (C) and providing him with means configured to authenticate the client to an anonymous certification authority (ACA)" (column 2, lines 57-62) as users and Service Providers that wish to make use of the Online Brokering Service initially register with the Brokering Service, and in turn provided with the client and server software components needed to make use of the Brokering Services.

In addition, Teper teaches the limitation of "authenticating the client to the anonymous certification authority using the means provided in step i) and supplying the client with means configured to enable the client to authenticate the client anonymously to a server (Se)" (column 2, line 62 – Column 3, line 4) as users provide various account information to the Online Broker. This information is maintained in a brokering database at the Online Broker site, and is not exposed to the Service Providers (SP). Each user additionally selects a password, and is assigned a unique ID which can be mapped to the user only by the Online Brokering Service. The password and unique ID are stored in the brokering database, and are used to authenticate registered users. Where, (column 5, lines 26-37) users are in turn provided with the software component needed to make use of the services offered by the broker providing the features of a pass-through authentication protocol which allows the registered user to be authenticated by the Online Broker upon accessing a Service Provider site while remaining anonymous to the Service Providers and the other entities of the distributed network.

Finally, Teper teaches the limitation of "authenticating the client by producing an anonymous signature and opening and maintaining an anonymous authentication session with a server (Se)" (column 3, lines 5-13) wherein a unique anonymous signature is used for each session (col. 11, lines 27-33) as when a user connects to a registered SP site and attempts to access an online service, the SP site initiates a challenge-response authentication sequence which allows the Online Brokering Service to authenticate the user for the SP site. Furthermore, (column 3, lines 31-34) upon determining that a user is authentic, the Online Brokering Service preferably sends an anonymous session ID to the SP site to allow the SP site to anonymously bill the user for services subsequently purchased.

It is noted, however, that Teper does not explicitly teach the limitation of "selectively allowing contact between the server (Se) and the anonymous certification authority (ACA) to revoke the anonymity of the client (C) using the signature provided in step iii)."

On the other hand, Camnisch teaches the abovementioned limitation (page 3, paragraph 0028) as none of the credentials reveal any information about the user's real identity or pseudonym. However, the showing of credentials can be carried out in such a way that a designated revocation manager can later find the user's identity and/or pseudonym.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Camnisch into the system of Teper to allow the

service provider to reveal a real identity of the user if needed for further prosecution (Camnisch, page 3, paragraph 0028).

As per claim 2, Teper teaches communication between the anonymous certification authority (ACA) and the server (Se), before the authenticating of the client to the anonymous certification authority, whereby the server (Se) presents to said authority (ACA) a request to obtain means enabling verification of the anonymous authentication supplied by a client (C)" (column 6, lines 14-20) as the Service Provider registers with the Broker by providing various business and payment information, and by entering a contract with the Broker. The Broker issues a password to the Service Provider, and provides a Service Provider with the server-side software components of the system.

As per claim 3, Teper teaches a first stage in which the client (C) calculates data formed of a series of tokens [interleaving bits of the password and bits of the random challenge message; col. 9, line 67-col. 10, line 1], wherein one of the series of tokens is configured to enable a session to be opened and others of the series of tokens are configured to enable the session to be maintained (col. 11, lines 10-12), a second stage in which the client makes a strong undertaking to the server as to the series of tokens (col. 10, lines 64-65)", and "a third stage of maintaining the session with the aid of the series of tokens (col. 11, lines 10-12).

As per claim 4, Teper teaches the series of tokens are configured for one-time use [each session; unique by pseudo random challenge seeds] and each of the series of token are strongly interdependent (col. 10, lines 1-5).

As per claim 5, Teper teaches the series of tokens are calculated using two cryptographic primitives (col. 10, lines 1-15).

As per claim 7, Teper teaches the second stage includes obtaining an anonymous signature of an initialization token enabling authentication of a client by the server (col. 11, lines 1-5).

As per claim 8, Teper teaches a numerical value is associated with the initialization token [message is represented by bits; col. 10, line 1).

As per claim 9, Teper teaches on each new authentication the client sends the server a token of at least one unit lower rank than that previously used (col. 9, lines 61-62).

As per claim 10, Teper teaches on each new authentication the client (C) sends the server a token whose rank is selected to be representative of the value of an operation (col. 9, lines 61-62).

As per claim 20, Teper teaches wherein the first stage calculates the series of token based on two cryptographic primitives, wherein the two cryptographic primitives are a hashing function (col. 10, lines 1-3) and a random number (col. 9, line 59).

Claim 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Teper in view of Camnisch as applied to claim 1 above, and further in view of Aiello et al. (US 6,397,329 B1).

As per claim 6, Teper teaches various ways of cryptographically constructing the challenge response. Teper teaches the first token is obtained by applying the hashing functions to the random number (col. 10, lines 1-2). However, Teper is silent in explicitly disclosing the second token is obtained by applying the hashing function to the first token obtained, and so on until n tokens are obtained: H(Wo) = Wi H(Wn-I) = W. Aiello teaches a secure way of hashing in this manner (see abstract). It is obvious to substitute known methods which yield predictable results to one of ordinary skill in the art. Using multiple hashes decreases the likelihood of being able to gain any protected information.

Claims 11, 12, 13, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Teper in view of Camnisch as applied to claim 1 above, and further in view of Sako (US 2001/0011351 A1).

With respect to claim 11, it is noted that neither Teper nor Camnisch teach the limitation of "it is applied to bidding and the steps of the client (C) submitting an increased bid are effected by sending successive tokens of lower rank"

On the other hand, Sako teaches the abovementioned limitation (page 4, paragraph 0069) as in the case where this anonymous participation authority management system is applied to a bidder management system of electronic bidding; the participant subsystem corresponds to a bidder subsystem and each eligible bidder

is given secret information from the manager subsystem beforehand and the reception subsystem performs bidding reception.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Sako into the system of Teper and Camnisch to provide additional functionality such as bidding application.

With respect to claim 12, it is noted that neither Teper nor Camnisch explicitly teach the limitation of "using a group signature by associating a plurality of identifiers and respective private keys with a single group public key." However, it is obvious that Teper must use some kind of encrypted channel between the broker and the server. This could act as a group key covering all the registered clients.

On the other hand, Sako teaches the abovementioned limitation (page 1, paragraph 0015) as the verification subsystem confirms that the data submitted has a signature verifiable by a group public key affixed and when the confirmation is obtained, this can be regarded as the data sent by a participant subsystem belonging to an eligible group.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Sako into the system of Teper and Camnisch because use of the group signature makes it impossible to identify the particular participant in the group, which makes it possible to maintain anonymity.

With respect to claim 13, it is noted that neither Teper nor Camnisch explicitly teach the limitation of "using a blind signature."

On the other hand, Sako teaches the abovementioned limitation (page 1, paragraph 0005) as a participant subsystem authorized to vote proves before a manager subsystem that the presenter is authorized to vote and then has the manager subsystem sign the voting contents by section of blind signature.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Sako into the system of Teper and Camnisch because since blind signature is used, even the manager subsystem cannot know to which participant subsystem the voting statement with the signature has been issued, which makes it possible to maintain anonymity.

As per claim 21, Teper is silent in explicitly teaching the rank is representative of a number of bid increments.

On the other hand, Sako teaches the abovementioned limitation (page 4, paragraph 0069) as in the case where this anonymous participation authority management system is applied to a bidder management system of electronic bidding; the participant subsystem corresponds to a bidder subsystem and each eligible bidder is given secret information from the manager subsystem beforehand and the reception subsystem performs bidding reception.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Sako into the system of Teper and Camnisch to provide additional functionality such as bidding application.

Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Teper in view of Camnisch and Sako as applied to claim 12 above, and further in view of Beaver et al. (US 7,234,059 B1), hereinafter Beaver.

It is noted that neither of Teper, Camnisch, and Sako explicitly teach the limitation of "the powers to revoke anonymity is shared between two or more authorities."

On the other hand, Beaver teaches the abovementioned limitation (column 2, lines 60-64) as in systems providing revocable anonymity, anonymity is in place unless a specified event (e.g., court order) demands it be revoked and the identity of the offender revealed.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Beaver into the system of Teper, Camnisch, and Sako to prevent undesirable situations in which troublemakers can act without fear of detection.

Claims 15 and 16 are rejected under 35 U.S.C. 103 as being unpatentable over Teper.

As per claim 15, Teper teaches a system adapted to open and maintain an authentication session guaranteeing non-repudiation, wherein an anonymous signature

unique to the session (col. 11, lines 27-30) and comprising a series of tokens is used to open and maintain each session (col. 9, line 60-col. 10, line 2), the system comprising:

means configured to implement three stages:

a first stage in which a client calculates the series of tokens, one of the series of token is configured to enable a session to be opened and another of the series of tokens is configured to enable the session to be maintained (col. 9, line 67 - col. 10, line 1);

a second stage in which the client makes a strong undertaking to the server as to the series of tokens (col. 9, lines 60-62);

a third stage of maintaining the session with the aid of the series of tokens (col. 11, lines 27-30). It is obvious that the series of tokens need to be present in order to initiate the authentication. Therefore the tokens aid in the creation of the anonymous signature in and as a result are indirectly responsible in maintaining the session because without them it could never have been initiated.

As per claim 16, Teper teaches wherein the first stage calculates the series of token based on two cryptographic primitives, wherein the two cryptographic primitives are a hashing function (col. 10, lines 1-3) and a random number (col. 9, line 59).

Claims 17 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Teper in view of Sako.

As per claim 17, it is noted that Teper does not explicitly teach the limitation of "using a group signature by associating a plurality of identifiers and respective private keys with a single group public key." However, it is obvious that Teper must use some kind of encrypted channel between the broker and the server. This could act as a group key covering all the registered clients.

On the other hand, Sako teaches the abovementioned limitation (page 1, paragraph 0015) as the verification subsystem confirms that the data submitted has a signature verifiable by a group public key affixed and when the confirmation is obtained, this can be regarded as the data sent by a participant subsystem belonging to an eligible group.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Sako into the system of Teper because use of the group signature makes it impossible to identify the particular participant in the group, which makes it possible to maintain anonymity.

With respect to claim 18, it is noted that Teper does not explicitly teach the limitation of "using a blind signature."

On the other hand, Sako teaches the abovementioned limitation (page 1, paragraph 0005) as a participant subsystem authorized to vote proves before a manager subsystem that the presenter is authorized to vote and then has the manager subsystem sign the voting contents by section of blind signature.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Sako into the system of Teper because since blind

signature is used, even the manager subsystem cannot know to which participant subsystem the voting statement with the signature has been issued, which makes it possible to maintain anonymity.

Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Teper in view of Beaver.

It is noted that Teper does not explicitly teach the limitation of "the powers to revoke anonymity is divided between two or more authorities."

On the other hand, Beaver teaches the abovementioned limitation (column 2, lines 60-64) as in systems providing revocable anonymity, anonymity is in place unless a specified event (e.g., court order) demands it be revoked and the identity of the offender revealed.

It would have been obvious to one of the ordinary skill in the art at the time of the invention to incorporate teachings of Beaver into the system of Teper to prevent undesirable situations in which troublemakers can act without fear of detection.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is

(571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/Syed Zia/

Primary Examiner, Art Unit 2431